Electronic Version
Stylesheet Version v1.1.1

# Claims

[c1] A smartcard transaction system configured with a biometric security system, said system comprising:
a smartcard configured to communicate with a reader;
a reader configured to communicate with said system;
a vascular scan sensor configured to detect a proffered vascular scan sample, said vascular scan sensor configured to communicate with said system; and,
a device configured to verify said proffered vascular scan sample to facilitate a transaction.

[c2] The smartcard transaction system of claim 1, wherein said sensor is configured to communicate with said system via at least one of a smartcard, a reader, and a network.

[c3] The smartcard transaction system of claim 1, wherein said vascular scan sensor is configured to facilitate a finite number of scans.

[c4] The smartcard transaction system of claim 1, wherein said vascular scan sensor is configured to log at least one of a detected vascular scan sample, processed vascular scan sample and stored vascular scan sample.

[c5] The smartcard transaction system of claim 1, further including a database configured to store at least one data packet, wherein said data packet includes at least one of proffered and registered vascular scan samples, proffered and registered user information, terrorist information, and criminal information.

[c6] The smartcard transaction system of claim 5, wherein said database is contained in at least one of the smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

[c7] The smartcard transaction system of claim 6, wherein said remote database is configured to be operated by an authorized sample receiver.

[c8] The smartcard transaction system of claim 1, wherein said vascular scan sensor device is configured with at least one of an optical scanner, x-ray, ultrasound, computed topography and thermal scanner.

[c9] The smartcard transaction system of claim 1, wherein said vascular scan sensor is configured to detect and verify vascular scan characteristics including biometric reference points and blood pressure characteristics.

[c10] The smartcard transaction system of claim 9, wherein

said biometric reference points include at least one of vascular coordinates, vascular lengths, widths and depths, and tissue lengths, widths and depths.

[c11] The smartcard transaction system of claim 9, wherein said blood pressure characteristics include at least one of waveforms, dicrotic notches, diastolic pressure, systolic pressure, anacrotic notches, and pulse pressure.

[c12] The smartcard transaction system of claim 1, wherein said vascular scan sensor device is configured to detect and verify false vascular and thermal patterns.

[c13] The smartcard transaction system of claim 1, further including a device configured to compare a proffered vascular scan sample with a stored vascular scan sample.

[c14] The smartcard transaction system of claim 13, wherein said device configured to compare a vascular scan sample is at least one of a third-party security vendor device and local CPU.

[c15] The smartcard transaction system of claim 13, wherein a stored vascular scan sample comprises a registered vascular scan sample.

[c16] The smartcard transaction system of claim 15, wherein said registered vascular scan sample is associated with

at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c17] The smartcard transaction system of claim 16, wherein different registered vascular scan samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

[c18] The smartcard transaction system of claim 16, wherein a vascular scan sample is primarily associated with first user information, wherein said first information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein a vascular scan sample is secondarily associated with second user information, wherein said second user informa-

tion comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein said second user information is different than said first user information.

[c19] The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered vascular scan sample.

[c20] The smartcard transaction system of claim 1, wherein said smartcard is configured to deactivate upon rejection of said proffered vascular scan sample.

[c21] The smartcard transaction system of claim 1, wherein said sensor is configured to provide a notification upon detection of a sample.

[c22] The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction.

[c23] The smartcard transaction system of claim 1, wherein

said device configured to verify is configured to facilitate the use of at least one secondary security procedure.

[c24] A method for facilitating biometric security in a smart-card transaction system comprising: proffering a vascular scan to a vascular scan sensor communicating with said system to initiate verification of a vascular scan sample for facilitating authorization of a transaction.

[c25] The method for of claim 24, further comprising registering at least one vascular scan sample with an authorized sample receiver.

[c26] The method of claim 25, wherein said step of registering further includes at least one of: contacting said authorized sample receiver, proffering a vascular scan to said authorized sample receiver, processing said vascular scan to obtain a vascular scan sample, associating said vascular scan sample with user information, verifying said vascular scan sample, and storing said vascular scan sample upon verification.

[c27] The method of claim 24, wherein said step of proffering includes proffering a vascular scan to at least one of an optical scanner, x-ray, ultrasound, computed tomography, and thermal scanner.

[c28] The method of claim 24, wherein said step of proffering

further includes proffering a vascular scan to a vascular scan sensor communicating with said system to initiate at least one of: storing, comparing, and verifying said vascular scan sample.

[c29] The method of claim 24, wherein said step of proffering a vascular scan to a vascular scan sensor communicating with said system to initiate verification further includes processing database information, wherein said database information is contained in at least one of a smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

[c30] The method of claim 24, wherein said step of proffering a vascular scan to a vascular scan sensor communicating with said system to initiate verification further includes comparing a proffered vascular scan sample with a stored vascular scan sample.

[c31] The method of claim 30, wherein said step of comparing includes comparing a proffered vascular scan sample to a stored vascular scan sample by using at least one of a third-party security vendor device and local CPU.

[c32] The method of claim 30, wherein said step of comparing includes comparing vascular scan characteristics including at least one of biometric reference points and blood

pressure characteristics.

[c33] The method of claim 24, wherein said step of proffering a vascular scan to a vascular scan sensor communicating with said system further comprises using said vascular scan sensor to detect at least one of false vascular and thermal patterns.

[c34] The method of claim 24, wherein said step of proffering a vascular scan to a vascular scan sensor communicating with said system to initiate verification further includes at least one of detecting, processing and storing at least one second proffered vascular scan sample.

[c35] The method of claim 24, wherein said step of proffering a vascular scan to a vascular scan sensor communicating with said system to initiate verification further includes the use of at least one secondary security procedure.

[c36] A method for facilitating biometric security in a smart-card transaction system comprising:
detecting a proffered vascular scan at a sensor communicating with said system to obtain a proffered vascular scan sample;
verifying the proffered vascular scan sample; and
authorizing a transaction to proceed upon verification of the proffered vascular scan sample.

[c37] The method of claim 36, wherein said step of detecting further includes detecting a proffered vascular scan at a sensor configured to communicate with said system via at least one of a smartcard, reader, and network.

[c38] The method of claim 36, wherein said step of detecting a proffered vascular scan includes detecting a proffered vascular scan at least one of an optical scanner, x-ray, ultrasound, computed tomography, and thermal scanner.

[c39] The method of claim 36, wherein said step of detecting includes at least one of: detecting, storing, and processing a proffered vascular scan sample.

[c40] The method of claim 36, wherein said step of detecting further includes receiving a finite number of proffered vascular scan samples during a transaction.

[c41] The method of claim 36, wherein said step of detecting further includes logging each proffered vascular scan sample.

[c42] The method of claim 36, wherein said step of detecting further includes at least one of detecting, processing and storing at least one second proffered vascular scan sample.

[c43] The method of claim 36, wherein said step of detecting

further includes using said vascular scan sensor to detect at least one of false vascular and thermal patterns.

[c44] The method of claim 36, wherein said step of verifying includes comparing a proffered vascular scan sample with a stored vascular scan sample.

[c45] The method of claim 44, wherein said step of comparing a proffered vascular scan sample with a stored vascular scan sample comprises storing, processing and comparing at least one vascular scan characteristic including biometric reference points and blood pressure characteristics.

[c46] The method of claim 44, wherein comparing a proffered vascular scan sample with a stored vascular scan sample includes comparing a proffered vascular scan sample with a biometric sample of at least one of a criminal, a terrorist, and a cardmember.

[c47] The method of claim 36, wherein said step of verifying includes verifying a proffered vascular scan sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.

[c48] The method of claim 36, wherein said step of verifying includes verifying a proffered vascular scan sample using

one of a local CPU and a third-party security vendor.